MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Common Bow Tie Errors and How the CCPS Concept Book Rectifies

Tatiana Norman
DNV GL USA, Inc.
1400 Ravello Drive
Katy, Texas 77449, USA
Email: tatiana.norman@dnvgl.com

Keywords: Bow tie; Hazard Identification; Risk Analysis; Human Factors

Abstract

The bow tie risk analysis method is growing in its application as it is a powerful tool for visually communicating major accident risks and the barriers deployed to prevent or mitigate these. The ease of communication can mislead users to think that bow tie creation is also easy. A new CCPS Concept Book, Bow Ties in Risk Management, thoroughly reviews how to create bow ties and provides detailed guidance on how to avoid errors.

This paper provides several examples of common errors seen in the current bow ties. These cover structural errors, such as degradation factors and controls are misplaced onto main pathways, barriers that do not comply with guidance on required barrier core attributes, and incorrect hazards, top events, and consequences. The paper also covers a better means to treat human error.

A final part of the paper presents a novel multi-level approach to bow ties that can be helpful for human error and mechanical integrity applications where deeper degradation controls are important to display.

Abbreviations

CCPS	Center for Chemical Process Safety
EI	Energy Institute
HAZOP	Hazard and Operability Study
HOF	Human and Organizational Factors
LOTO	Lock Out Tag Out

Introduction

Bow tie analysis has been used for many years and is growing in its application as it is a powerful tool for visually communicating major accident risks and the barriers deployed to prevent or mitigate these. The ease of communication can mislead users to think that bow tie creation is also easy, and this is not the case. The method is qualitative and uses a diagrammatic representation of major accident threat and consequence pathways showing the hazard, top event, threats and consequences, with intervening barriers and degradation factor pathways linked to the main pathway barriers. A unique feature of the bow tie is its ability to communicate complex major hazard events in a simple format that is easily communicated to all members of staff, contractors, regulators and other stakeholders. Bow ties require a significant effort to create and update as necessary. A new CCPS Concept Book (CCPS & EI, 2018) thoroughly reviews creation of bow ties and provides detailed guidance on avoiding errors.

One of the primary goals of the book is to ensure consistent application of the bow tie technique by defining structural elements together with good and poor examples for clarification. An issue with bow ties is that there is no widely accepted methodology or definitions and this has resulted in many inconsistencies, poor structures, and poor treatment of human and organizational factors. CCPS along with the Energy Institute, collaborated to provide a book that compiles current practices and provided a set of suggested approaches.

The basic bow tie is shown in Figure 1. The figure shows the 8 main bow ties elements: 1) hazard, 2) top event, 3) consequence, 4) threat, 5) prevention barrier, 6) mitigation barrier, 7) degradation factor, and 8) degradation control.

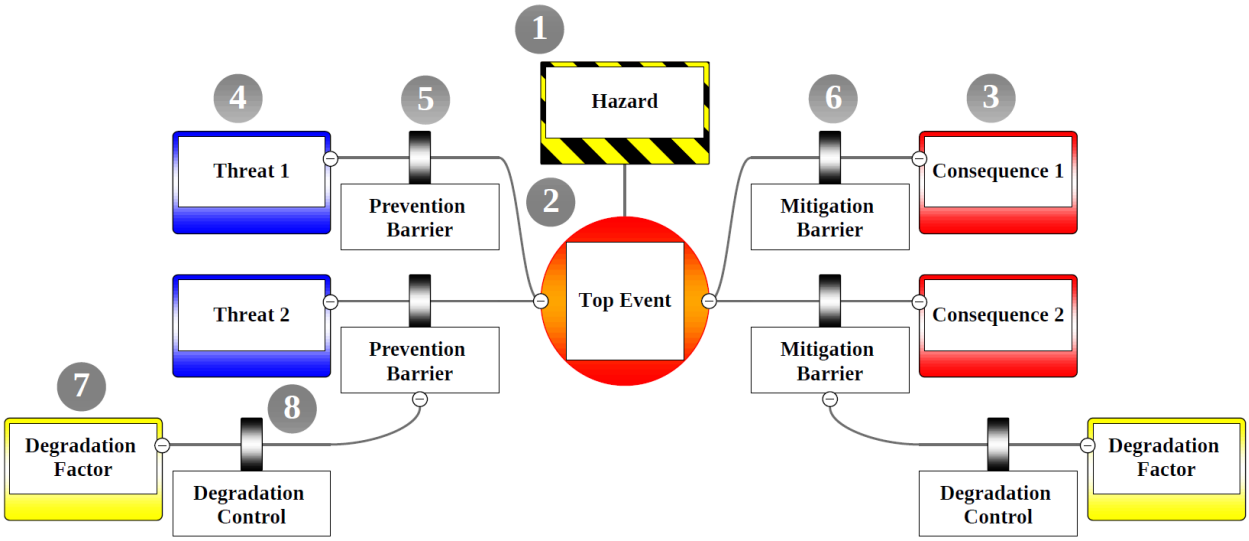


Figure 1. Basic Bow Tie

Common Errors: Hazard and Top Event

Hazard

Hazard is defined in the book as an operation, activity or material with the potential to cause harm. It appears at the top of the bow tie diagram and is the source of the risk. It is important

that the hazard is defined properly as this is the basis for the entire bow tie diagram. Generic hazards can lead to generic bow ties and lack the necessary detail.

A common error of bow tie is a hazard that is too vague. For example, specifying 'Chlorine' alone as the hazard would be too generic of a description. A better example would be 'Chlorine stored in a tank' as in Figure 2. Hazards should be formulated in a controlled state and not the loss of control of the hazard (this is the top event) or the actual harm (the consequences). CCPS/EI suggest the reader ask "Is the hazard as described part of our normal business?"

Figure 2. Example Hazard

Another common error is a hazard that does not link to the consequences listed. It is important to include enough detail in the hazard box to ensure the correct consequences are listed. The hazard box on the bow tie diagram cannot show all the details of the hazard but the specifics should be documented. The common theme from the CCPS/EI book is that the hazard should be defined as specific as possible and ensure that it links to the Top Event.

The book provides a table of well-defined and poorly defined hazards. A few examples are given in Table 1 below.

Table 1. Well-defined and Poorly-defined Hazards (CCPS/EI 2018)

Hazard	**Commentary**
Working at height (>2m) on formwork	Working at height is a common hazard and specifying the height provides additional detail.
Pressurized propane storage in sphere	The normal operational state is defined and some context of the volume is indicated.
H_2S	The hazard does not properly set the scope nor identify the scenario that will be analyzed. The bow tie will be different depending on the controlled state of the H_2S (e.g. drilling into formation containing H_2S, smelting iron with H_2S as by-product, or working in sewers where H_2S is present).
Control System Failure	This can be a top event, threat or a barrier failure depending on the context. It does not specify the actual hazard – perhaps 'hydrocarbons in formation'.

Top Event

The top event is the moment when control over the hazard or its containment is lost. Common generic top events include loss of containment, loss of separation, loss of stability or loss of control. The top event should be linked to the hazard. If the hazard is gasoline stored in tank and good example for top event could be tank overflow.

The top event should not be a consequence (e.g. explosion). A common error in defining a top event is to choose a consequence with damage or harm rather than a loss of control event. CCPS & EI (2018) recommend asking the question, "Is this loss of control or is this a consequence?" Another common error is choosing a top event that is part of an event sequence (e.g. ignition).

Good practice is to define a top event where multiple threats and consequences can be identified. If the top event is too narrow you run the risk of needing several diagrams to cover the risks surrounding your asset or operations. On the contrast, the top event should not be too broad. Building more than ten threats and consequences for a single top event could be too broad. The balance between detail and economy should be influenced by the intended audience, the objective of the study or historical incidents.

Common Errors: Consequence and Threat

Consequence

After defining the top event, the next step is to determine the consequences. A common mistake is defining treats before consequences since this would be the natural progression given the way the bow tie is drawn. The book suggests defining consequences before threats as this will help the team later define only the threats that acting on the hazard can lead to significant consequences. Consequences are unwanted outcomes that could result from the top event and lead to damage or harm.

CCPS & EI (2018) suggest describing the consequence as '[Damage] due to [Event]'. By describing the consequence this way, different barriers can be required to stop or mitigate damage depending on the event leading to the damage. For example, 'fatalities due to fire' might call for different mitigation barriers than 'fatalities due to toxic gas'. Consequences can be chosen which are good or poor, but generally selecting consequences is less prone to error than some other bow tie elements. Table 2 provides a few examples of poorly worded consequences.

Table 2. Common Consequence Errors

Top event	One Consequence	Comment – why this is poorly worded
Gasoline tank overflow	Environmental damage or Pollution	The consequence links directly to the top event but it is vague, and not specific as to the nature or severity of the environmental damage. Is the damage to land or water (small stream or large river?) or to specific species? Consequences should name the receptor affected. Inclusion of the scale is useful to design an adequate response from the mitigation barriers.
Loss of control over the vehicle	Crash barrier damage	This is a possible consequence, but it is likely to be unimportant compared to other consequences and might be better grouped (e.g. 'asset damage to car and road infrastructure').

Threat

Threats are possible initiating events that can result in a loss of control or containment of a hazard. The threat must lead to the top event if the pathway is not prevented. Three categories are helpful to initiate discussion in identifying threats:

1. primary equipment not performing within normal operating limits (mechanical fault),
2. environmental influence (overpressure due to solar heating of blocked in pipeline),
3. operational issues (insufficient personnel present to support all required human barriers during start-up).

Using 'human error' as a threat is not recommended by CCPS/EI as this commonly leads to structural errors in the bow tie. A structural error in a bow tie means that some important rule for bow tie construction has been violated. This is topic is elaborated more in a later section of the paper.

A frequent mistake is to exclude threats that will rarely lead to the top event because of the argument that there are already many prevention barriers in place to control this threat. Every credible threat should be added to facilitate decisions as to whether there are enough prevention barriers in place to control the particular threat and visualizing the credible threats enables a more complete overview. Threats should have a direct causation and be specific. Identifying direct threats will often result in inclusion of more specific barriers compared to indirect threats. They should also be sufficient and not barrier failures. If a threat can only cause the tope event in combination with another threat, it is not sufficient and therefore incorrect. Table 3 provides a few examples of poorly worded threats.

Table 3. Common Threat Errors

Threat	Top event	Comment – why this is poorly worded
Level gauge out of preventive maintenance cycle	Tank overflow	The threat is not a direct cause of tank overflow just because it is late on a preventive maintenance cycle. The threat is excess flow into the tank and the barrier is associated with operator vigilance using the level gauge.
Failure of anti-lock braking system (ABS)	Loss of control over the car	This is a safety system which has failed. It does not cause the top event on its own. A better threat would be a sudden burst tire.

Common Errors: Barriers

The most common error often found on a bow tie diagram is with barriers. CCPS & EI define barrier as a control measure or grouping of control elements that on its own can prevent a threat developing into a top event (prevention barrier) or can mitigate the consequences of a top event once it has occurred (mitigation barrier). A barrier must be effective, independent, and auditable. This provides confidence that it will be able to act when required and as intended, without any action or intervention external to the barrier, and that its degradation will be prevented. The book differentiates between barriers and degradation controls. Barriers appear on the main pathway (threat to top event or top event to consequence) and degradation controls only appear on degradation pathways and serve to support main pathway barriers against degradation. The biggest mistake found on bow tie diagrams is mistaking degradation controls as barriers. For example, training and competence are not barriers but are however degradation controls. Training competence may support a particular barrier but are not capable of preventing a top event or mitigating the consequences. Effective, independent and auditable are explored furthered in the next sections.

Effective

A barrier is effective is it performs the intended function when demanded and to the standard intended. A common mistake when representing effective barriers on a bow tie include identifying incomplete barriers, like fire and gas detection. While these are important barriers they rely on other elements to completely stop the scenario from developing further. The book suggests a complete barrier could be fire and gas detection, automatic logic controller (or human response to alarm) and ESD.

Independent

Barriers should be independent of the threat and or other barriers on that pathway. For example, if the threat is loss of power a barrier requiring power to operate would not be permissible. The barrier is not independent of the threat. Also, it is important that there is as little common mode failure between barriers as possible. It is often difficult to find barriers that have no common mode and for this reason it is not necessary to remove barriers with some minor aspect of common mode. The book suggests managing the risk of a plausible common mode failure by the adding other

barriers that do not have that common mode. Adding different types of barriers is advisable and usually can help avoid some general common mode failures.

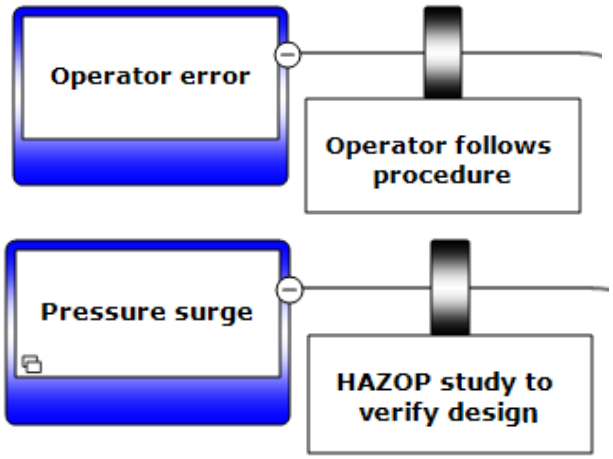
Auditable

Barriers should be capable of being audited to check that they work when called upon.

The most common mistakes regarding barriers are:

- displaying multiple barriers that are actually elements of a single barrier;
- barrier titles that are not informative;
- placing barriers on the wrong side of the top event; and
- indicating measures which are not barriers.

The figures below are further examples of common errors and remedies.



Threat and barrier are not independent

HAZOP study is not a barrier

Figure 3. Incorrect Barrier Examples

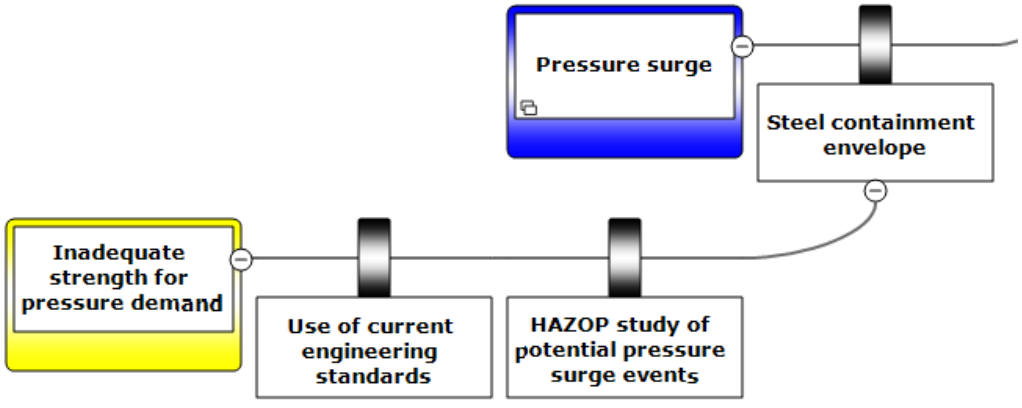


Figure 4. Better Barrier Examples

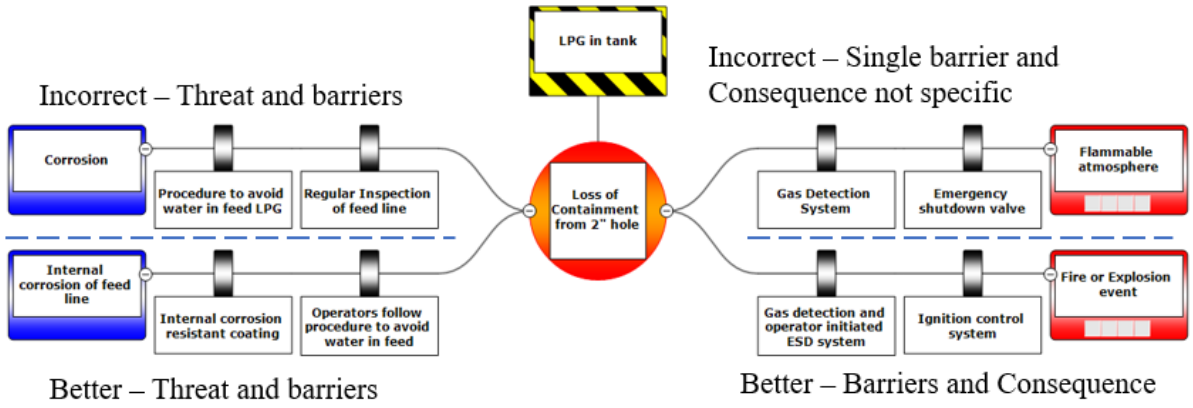


Figure 5. Incorrect and Better Barrier Examples

In summary, the list below provides some dos and don'ts regarding barriers on the bow tie diagram:

- Effective / Independent / Auditable
- If active – must display all elements of Detect – Decide – Act
- Should not be degradation controls
- If prevention side – must be able to stop Top Event
- If Mitigation side – must significantly mitigate consequence
- A procedure is NOT a barrier, but an operator executing a procedure is
- Similarly, a warning sign is not a barrier
- Systems are usually not barriers
- Inspection and Maintenance are usually not barriers
- Lock out tag out (LOTO) and Work Permit are usually not barriers
- HAZOP review is not a barrier
- A trivial control is not a barrier

Treatment of Human Error in Bow Ties

The CCPS and the Energy Institute recognized the need to address the current inconsistencies in the treatment of Human and Organizational Factors (HOF) in bow ties as this could significantly improve process safety. In bow ties, HOF issues can appear in several places. Humans (including human failure – error or inaction) can be modeled a threat, but more often appear either i) as part(s) of a prevention or mitigation barrier, ii) as a degradation factor, or iii) as part(s) of a degradation factor control. Therefore, humans can form a barrier or a barrier element. Since a human barrier is always active, it must have all elements of 'detect-decide-act' present (CCPS & EI, 2018).

The term 'human error' has sometimes been used as a main pathway threat. However, the required barriers can be very different based on the type of human error and the context in which it might occur. Degradation controls against a slip (e.g., fatigue management) would be different to a mistake (e.g., refresher training). The term 'human error' is usually too imprecise to be a good main pathway threat - it should appear as a specific degradation factor linking through the degradation pathway to a main pathway barrier. The book recommends that human failure should not be used as a main pathway threat. Making human error a threat almost always results in structural errors to bow ties; mainly barriers that do not meet the validity criteria.

CCPS & EI (2018) found many organizations developed bow ties where HOFs were represented as a threat for a main pathway. For example, part a of Figure 6 shows adding catalyst to an exothermic reactor before proper mixing is established can lead to a runaway reaction and an explosion. Treating human error as a threat results in an incorrect analysis because:

1. The HOF fails to meet the definition of a threat as it lacks the ability to combine with the hazard to lead to a top event.
2. The resulting barriers "Training" and "Supervision" on the main pathway fail to meet the definition of barriers as they lack the ability on their own to prevent a threat developing into a top event and cannot detect-decide-act.
3. The resulting four barriers on the main pathway lead to overconfidence in control over the threat.

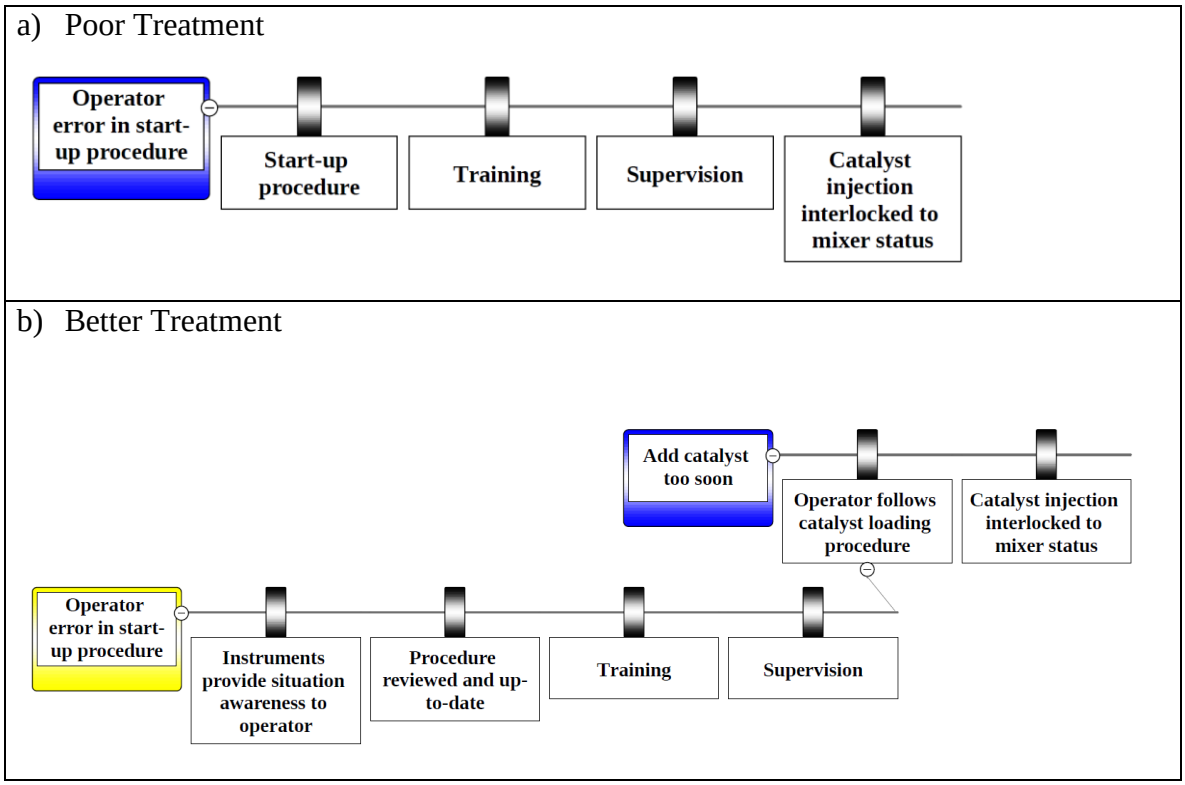


Figure 6. Example 1 Poor and Better Treatment of Human Error in Bow Tie

Treating human error as a degradation factor for a main pathway barrier is shown in part b of Figure 6 which results in a correct analysis because:

1. The HOF "Operator error startup procedure" as a degradation factor for the barrier "Operator follows catalyst loading procedure" meets the definition of being a situation, condition, defect, or error that compromises the function of a main pathway barrier, either through degrading it or reducing its effectiveness.
2. The resulting barriers "Training" and "Supervision" on the degradation factor pathway meet the definition of safeguards as they support the main pathway barrier and lie along degradation pathways into that barrier where they help defeat the degradation factor.
3. The resulting barrier "catalyst injection interlocked to mixer status" on the main pathway more correctly represent the control over the threat and the resulting four safeguards on the

degradation pathway more correctly represent the level of attention paid to maintaining the barrier “Operator follows catalyst loading procedure”.

Figure 7 provides another example of poor and better treatment of human error on bow ties.

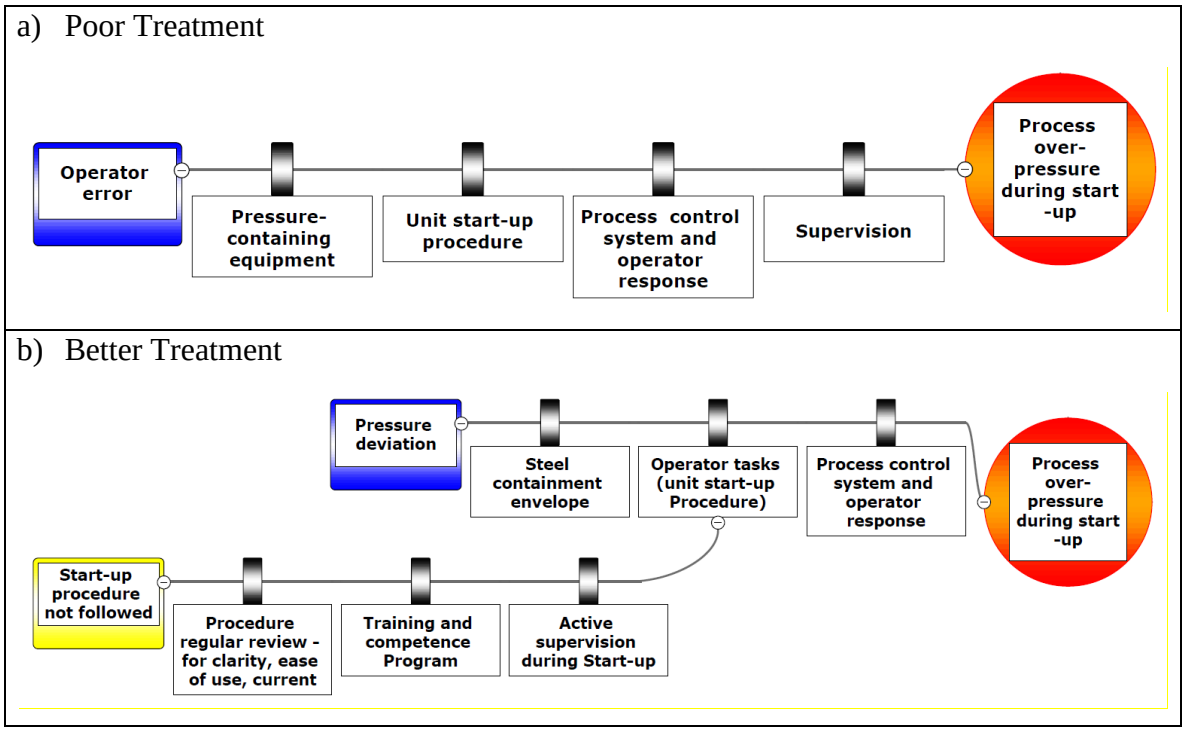


Figure 7. Example 2 Poor and Better Treatment of Human Error in Bow Tie

Defining Human and Organizational Factors in Bow ties

In Bow Ties in Risk Management two approaches to bow ties are presented: a conventional approach (standard bow tie) and a more advanced multi-level approach (multi-level bow tie). The multi-level approach is a new approach and offers potential benefits in addressing additional analysis of HOF. Multi-level bow ties can be a better approach to exploring human failure aspects in bow ties and can display a range of degradation controls. These would be deeper level controls supporting standard bow tie degradation controls against their own degradation.

In the multi-level approach, the standard bow ties main pathways and degradation factor pathways remain unchanged. The extension shows how degradation controls in the standard bow tie can be degraded and the additional controls that might be needed. This is shown in Figure 8. This extra level is defined as extension level 1. Degradation control examples at the standard bow tie level might include: procedures reviewed and up-to-date, training, and supervision; while extension level degradation controls might include: drug and alcohol testing, stop work authority, and senior management tours.

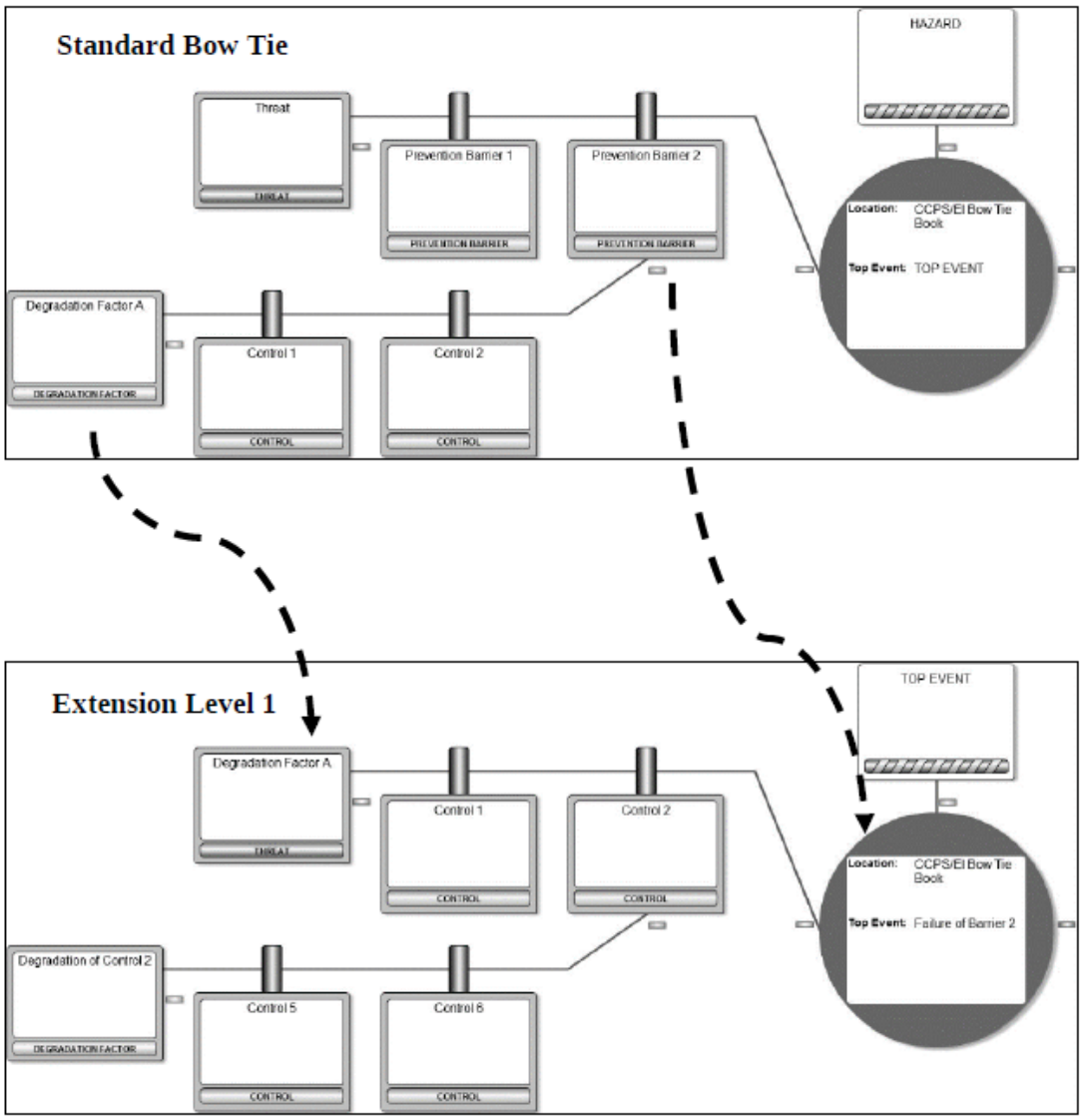


Figure 8. Concept of Multi-Level Bow Tie Approach (CCPS & EI, 2018)

Quality Checks

CCPS/EI identifies many matters to check, post workshop, in order that the final bow ties are useful and structurally correct. The list includes overall checks for items including consistent terminology, the right mix of people in the workshop and consistency with the agreed study terms of reference. There are several other quality checks for items pertaining to the bow elements themselves; for example, is the hazard clearly expressed with sufficient data or do all the main pathway barriers meet the validity criteria.

Conclusion

The bow tie method is a qualitative risk analysis method addressing major accident events and the key barriers and safeguards used to manage these. The method is growing in use in the process industries, for both upstream and downstream petro-chemical industries, as well as other major

hazard industries such as aviation, railways, and shipping. A bow tie can be a very powerful communication tool. The ease of communication can mislead users to think that bow tie creation is also easy. CCPS along with the Energy Institute, collaborated to provide a book that compiles current practices and provides a set of suggested approaches.

One of the primary goals of the book is to ensure consistent application of the bow tie technique by defining structural elements together with good and poor examples for clarification. This paper set out to highlight some of the common errors for the eight bow tie elements. The hazard should be specific and link to the top event. Typical top events include loss of containment or loss of control. Consequences should be described as '[Damage] due to [Event]'. Threats should have a direct causation and be specific. A majority of the mistakes are realized when defining barriers. A barrier must be effective, independent and auditable. Each individual barrier must have the capability to completely stop the threat from leading to the top event, or if a mitigation barrier, significantly reduce or eliminate the consequence. HOF has often been poorly treated in current bow ties. The book recommends that human failure should not be used as a main pathway threat. Multi-level bow ties were introduced as a method to better approach to exploring human failure aspects in bow ties and can display a range of degradation controls.

References

CCPS & EI (2018) *Bow Ties in Risk Management: A Concept Book for Process Safety*. American Institute of Chemical Engineers, John Wiley & Sons, New Jersey.